(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 January 2001 (04.01.2001)

PCT

(10) International Publication Number
WO 01/01644 A1

(51) International Patent Classification⁷: H04L 12/58

(21) International Application Number: PCT/KR00/00689

(22) International Filing Date: 29 June 2000 (29.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1999/25510 29 June 1999 (29.06.1999) KR

(71) Applicant: SAMSUNG ELECTRONICS CO., LTD. [KR/KR]; 416, Maetan-dong, Paldal-gu, Suwon-shi, Kyungki-do 442-370 (KR).

(72) Inventors: CHOI, Hee-Chang; #104-1304 Lucky Apt., Taehyon-dong, Sodaemun-gu, Seoul 120-757 (KR). KIM, Seong-Eun; #112-1501 Dalbitmaeul, Hwajong-dong, Dukyang-gu, Koyang-shi, Kyonggi-do 412-270 (KR).

(74) Agent: LEE, Keon-Joo; Mihwa Building, 110-2, Myongryun-dong 4-ga, Chongro-gu, Seoul 110-524 (KR).

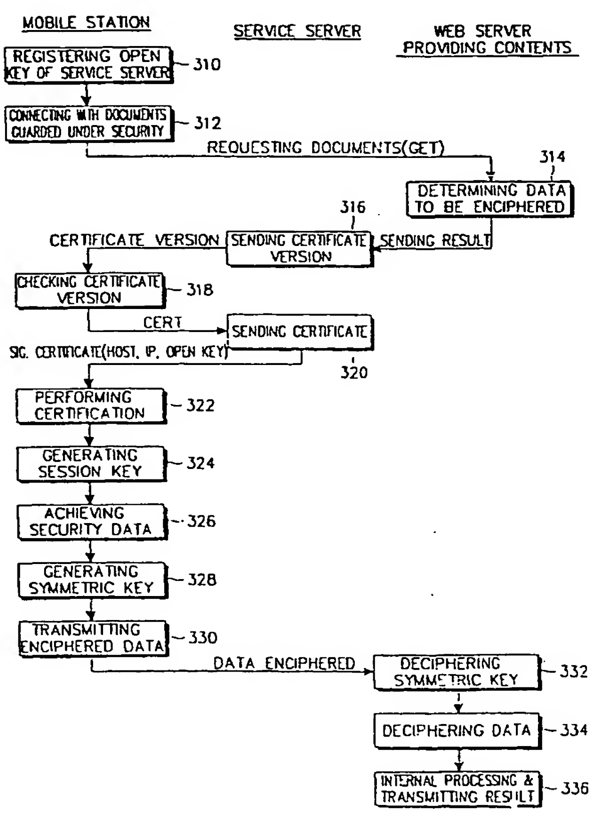
(81) Designated States *(national)*: BR, CN, IL, JP, SG, TR.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: APPARATUS FOR SECURING USER'S INFORMATION IN A MOBILE COMMUNICATION SYSTEM CONNECTED TO THE INTERNET AND METHOD THEREOF



(57) Abstract: An apparatus for securing the user's secret information transmitted from a mobile station is provided in a mobile communications system in communication with a web server through an Internet service server, wherein the data relating to the user's secret information is selected in response to the data request from the mobile station and/or web server, the selected data is enciphered in a given format, and the enciphered data is directly transmitted to the web server and/or the mobile station without any additional processing operation by the service server.

WO 01/01644 A1

APPARATUS FOR SECURING USER'S INFORMATION IN A MOBILE COMMUNICATION SYSTEM CONNECTED TO THE INTERNET AND METHOD THEREOF

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to an apparatus and method for securing the information of a subscriber in a mobile communication system in communication with the Internet.

2. Description of the related art

A recent development in the mobile communication has enabled users to execute the so-called electronic trade through the Internet using wireless communication technology. In order to foster the electronic trade on the Internet, the most important thing is to prevent the leakage of the personal information of a client while he or she is making a connection to the Internet web server, which provides electronic trade contents. Accordingly, the goal of the security system is to secure the personal information of the user while using the Internet so that an unwanted user can not tap into the personal information of the user, such as a password to access the web server, credit card number with its related password to make transaction, etc.

The conventional security system for securing confidential information used in the wired Internet communication typically employs a Secure Socket Layer (SSL), which is proposed by the Netscape Company in the United States. The SSL system encodes the information from a client in a known manner readable only by the web server. However, the SSL system may not be properly employed for the wireless or the mobile Internet communication system due to the reasons discussed below.

Firstly, the mobile station has a limited memory capacity that is inadequate to execute the web applications as in the SSL system. Thus, the conventional mobile station is not designed to execute such web applications. Secondly, in order to make a wireless connection to the Internet web server, the mobile station first has to be connected with the pertinent Internet service server to request the web content services. In this case, the security system between the web server and the service server should have the same standard as that of between the service server and the mobile station, in order to properly perform and protect personal information in the whole network. However, the conventional security system does not provide a uniform standard between

them. As an illustrative example, FIG. 1 depicts a conventional mobile communication network system provided in the conventional security system. As shown, the SSL system is employed between the service server and the web server, but a wireless security system with a different system is employed between the mobile station and the service server. Thus, the whole network does not have the same standard between them. Accordingly, the prior art security systems having different systems and standards can not properly provide the means for securing the personal information of the user.

As aforementioned, the conventional security system designed for the wired Internet communication system can not be properly applied to the wireless Internet communication system, thus impeding the booming market of the electronic trade through the Internet using mobile communication technology.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide an apparatus and method for securing confidential user information when executing electronic trade using the mobile Internet communication system, wherein the prior art system uses the SSL system employed in the wired Internet communications.

It is another object of the present invention to provide an apparatus and method for securing confidential information by achieving end-to-end security from a mobile station to a web server using the same standard to conduct the data flow between the mobile station, the service server, and the web server.

According to one aspect of the present invention, an apparatus for securing the user's secret information transmitted from a mobile station to a web server through an Internet service server is provided, wherein the data relating to the user's secret information is selected in response to the data request from the mobile station and/or web server, the selected data is enciphered in a given format, and the enciphered data is directly transmitted to the web server and/or the mobile station without further intervention by the service server.

The present invention will now be described more specifically with reference to the drawings attached only by way of example.

BRIEF DESCRIPTION OF THE ATTACHED DRAWINGS

FIG. 1 is a schematic diagram for illustrating the conventional mobile Internet communication system with the conventional mobile security system;

FIG. 2 is a schematic diagram similar to FIG. 1 and illustrates a mobile security system according to the present invention;

FIG. 3 is a schematic diagram for illustrating the procedure of transmitting an ordinary web document and the secret data according to the inventive security system in the mobile Internet communication; and,

FIG. 4 is a flow diagram for illustrating the process of securing the user's information according to the inventive mobile Internet communication.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

In the following description, for purposes of explanation rather than limitation, specific details are set forth such as the particular architecture, interfaces, techniques, etc., in order to provide a thorough understanding of the present invention. However, it will be apparent to those skilled in the art that the present invention may be practiced in other embodiments that depart from these specific details. For the purpose of clarity, detailed descriptions of well-known devices, circuits, and methods are omitted so as not to obscure the description of the present invention with unnecessary detail.

In order to provide a level of assurance that the purported sender of the message is in fact the true sender of the message, a digital/electronic signature can be encrypted using various known methods. The enciphering algorithm suitably applied according to the present invention is a Riverst-Shamier-Adleman (RSA) public key algorithm, which is the most widely used algorithm in the current electronic trade security system. The RSA algorithm provides both enciphering and electronic signatures (or encryption keys) based on prime factorization. That is, the principle of the RSA algorithm is based on the fact that it is easier to calculate the product of two prime numbers "p" and "q", but it is difficult to extract the "p" and "q" from the product "n", which is obtained by multiplying "p" and "q". That is, two keys, one being the public key and the second the secret key, are used so that whenever one encrypt something with the secret key, it can be decrypted only with the public key, and vice versa. In the embodiment of the present invention, the RSA algorithm generates the public key and secret key used for

enciphering/deciphering a session key. The public key is used by the client to encrypt the session key, which then sends the encrypted session key back to the server. The server decrypts the session key with its secret key and establishes the secured connection with the client.

Moreover, in the embodiment of the present invention, the algorithm for generating the session key uses a SEED symmetric key algorithm, which is based on the Korean Data Encryption Standard and uses the 128-bit block enciphering algorithm developed by the Korea Information Security Agency (KISA) for public electronic trade. The SEED symmetric algorithm features 8-, 16-, and 32-bit data processing, deciphering in the way of block enciphering, and the input/output phrase and input key is 128bits. It is also designed to safeguard against the Differential Cryptanalysis (DC)/ Linear Cryptanalysis (LC) and includes the enciphering/deciphering speed faster than three times that of the Data Encryption Standard (DES). Its structure is based on Feistel and the internal function is designed to use a look-up table obtained by converting a non-linear function. In the present invention, the SEED symmetric key algorithm is applied with 12 rounds to generate the session key by which the data of the user's information is enciphered.

The mobile station, the Internet service server, and the web server are operated according to the present invention in the mobile Internet communication as described below.

First, the mobile phone is provided with an inventive security program required for connecting with the web server to receive the public key and to internally generate the session key used during a security transaction. The session key is used to encipher and decipher the data. The enciphering is performed according to the RSA algorithm and the 128bits SEED algorithm. The web server, using the RSA algorithm, generates the public key and the secret key to enable the mobile station to perform the security transaction by sending the public key to the mobile station. The received public key is used to generate the session key to encipher the data transmitted by the mobile station, and the mobile station generates the session key using the SEED algorithm. Then, the web server uses the secret key to decipher the session key used to encipher the data transmitted by the mobile station. That is, the data encrypted using the public key can be decrypted only by using the secret key, and vice versa. Thus, the web server deciphers the session key, which is generated using the SEED algorithm, using the RSA secret key and the deciphered session key is used to decipher the enciphered data according to the

enciphering and deciphering of the 128bits symmetric key SEED.

According to the embodiment of the present invention, the data processing between the mobile station and the web server is initiated when the web server generates a pair of its own public key and secret key. The public key is sent to the service server, then revised and sent as a certificate to the mobile station upon a request. At this point, the mobile station has been authorized for use and the service sever acts as an intermediary between the mobile station and the web server by forwarding data as needed. Then, the mobile station stores the public key to internally generate a session key to encipher the confidential data to be sent to the web server. To generate the session key, the mobile station enciphers the received public key to generate the symmetric key to be sent to the web server. Thereafter, the web server deciphers the symmetric key with its own secret key. With the deciphered symmetric key, the web server deciphers the enciphered data received from the mobile station. In a reverse transmission, the web server enciphers data to be sent to the mobile station using the symmetric key received from the mobile station. The mobile station in return deciphers the enciphered data received from the web server using the symmetric key that is previously sent to the web server. In the embodiment of the invention, the service server is provided as a proxy server.

The data format on each path of the mobile Internet communication is described in connection with FIG. 2, wherein the security system among the mobile station, the service server, and the web server uses the inventive mobile micro security system (MMS). Namely, the same standard, MMS, is employed between the mobile station and the web server. As the public key of the web server is electronically signed with the secret key of the web server at the moment when the public key is first sent to the mobile station, the path between the mobile station and the mobile communication network can not be tampered by a hacker using the false public key. Moreover, the data packet enciphered by the mobile station is in the form of 128bits code so that the hacker can not comprehend the content of the original document. Furthermore, the hacker can not tap into the data packet as it travels from the mobile network to the service server via the Internet. This is achieved as the path between the mobile communication network and the service server makes the data packet, enciphered by the mobile station, in form of 128bits to the service server via the Internet, thus preventing a hacker from hacking its content.

In addition, the internal network of the service server is protected by a firewall

with a separate hacking-detective system according to the present invention. The service server simply transfers the enciphered data from the mobile station to the web server without any processing operation therein. Also, the service server and the web server are usually connected through an exclusive line through which the 128bits-enciphered data is transmitted, thus making it difficult for the hacker to access.

Furthermore, the hacking-detective system according to the present invention is realized because the web server receives the symmetric key randomized by the mobile station according to 128bits SEED algorithm. Then, the web server securely deciphers the 128bits-enciphered data received from the mobile station using the RSA secret key. In this way, the enciphered data of the mobile station may be deciphered only by the web server, and the enciphered data from the web server may be deciphered only by the mobile station. The latter is possible because the SEED symmetric key of the web server can also be transferred to the mobile station in a reverse operation.

Communication between the mobile station and the web server proceeds with each message enciphered by the session key before being sent and deciphered by the session key at the receiving end, wherein session key generated from the mobile station is enciphered using the public key and generated as symmetric key. To this end, the mobile station is installed with the security program for connecting with the security service server. The security program features a function to receive the public key from the web server and in return internally generates a session key to encipher personal information and is sent from the mobile station to the web server. That is, the session key is used to encipher and decipher the secret data according to the RSA enciphering and the 128bits SEED symmetric key.

FIG. 3 schematically shows the transmission of an ordinary web document without any enciphering and the transmission of secret data that is enciphered according to the present invention. Namely, the service server transmits an ordinary web document between the mobile station and the web server through a proxy server and transmits the personal data between them without any additional processing operation. As shown in FIG. 3, two different data transmission are operated according to the present invention due to the limited data amount that can be transmitted and processed in the wireless Internet communication. Thus, only the personal/secret data, which needs to be protected from an unwanted third party, is directly transmitted between the mobile station and the web server.

According to the embodiment of the present invention, the process of securing the user's information when the mobile station attempts to connect with the web server is described in connection with FIG. 4, wherein the mobile station registers the public key received of the service server, in step 310, which is hard-coated on the web browser of the mobile station. The service server registers the public key, certificate, and address of the web server along with its certificate version information, which are periodically revised according to the corresponding data delivered by the web server. In step 312, the mobile station requests a connection with the web page to receive electronic files in response to the user's request. This request is directly transmitted to the web server through the "GET" command for requesting the electronic document that can be accessed with the personal/secret information. At this time, the service server does not perform any additional processing operation to the GET command being transferred to the web server. Here, the web server may be a banking server, a stock dealing server, etc.

In step 314, the web server being requested with the connection determines the data to be enciphered upon receiving the request from the mobile phone, then informs the result to the mobile phone through the service server. The data to be enciphered includes personal/secret information, such as a password and a credit card number. Other data such as the user's login ID, ordinary character information, etc., does not require enciphering so that the amount of the data enciphered can be reduced. This is helpful because the mobile Internet communication is very limited in the amount of data that can be processed compared to the wired Internet communication. In step 316, the service server sends the presently registered certificate version, which periodically revised by the web server, to the mobile station. The certificate version provides updated information about the host name, the IP address, and the public key of the web server that can be used to authenticate message source. Then, the mobile station determines whether the received certificate version is the same as the previously registered version. The previously registered version is downloaded from the previous access to the same web server by the mobile station. If they are the same, the enciphering is performed with its previously registered version.

Alternatively, if not the same, the mobile station requests the service server to send a new version of certificate. The request is made by a "CERT" command, which is prearranged protocol between the mobile station and the service server for sending the certificate. In response to the command "CERT," the service server sends the presently registered certificate of the web server in step 320. That is, if there were a request for a new certificate version by the mobile station, the service server (or proxy server) having

the updated information that is periodically downloaded from the web server (content server), sends a response message, which is comprised of a header and a text. In the header, the digital SIGN (signature for the public key of the web server requested by the mobile station) is attached thereto, and the certificate (host name, IP address, and public key) is attached to the text portion.

In step 322, the mobile station receives the response message from the service server and authenticates the text of the certificate by validating the digital SIGN in the header. Namely, the mobile station checks whether the digital SIGN corresponds to that of the pubic key of the web server, and also checks for whether the text is damaged. If the digital SIGN is confirmed, the mobile station retrieves the public key included in the certificate and revises its certificate table therein. In step 324, the session key is generated using the public key contained in the certificate for the transmission of the user's information under security. As described above, the session key is generated according to the 128bits SEED algorithm, which is used to encipher the personal data to be transmitted by the mobile station user. In step 326, the user's information is enciphered by the session key to achieve the security data. In step 328, the session is enciphered by the public key to generate the symmetric key.

In step 330, the symmetric key obtained by enciphering the session key using the public key and the data enciphered by the session key are transmitted to the web server via the service server. Of course, the service server does not perform any further operation to the data being transmitted to the web server. Then, in step 322, the web server deciphers, using the secret key, the symmetric key included in the user's information received from the mobile station to generate a session key. In step 334, the web server deciphers, using the generated session key, the user's information, i.e., the security data enciphered by the mobile station so that the original data can be retrieved and the original data can be processed by the web server accordingly.

Meanwhile, in step 320, a hash is generated using a hash function (i.e., Message-Digest 5 (MD5). The MD5 is the functional protocol used for enciphering, of which, if the result agrees with the certificate, it is considered that the data transmission has been normally achieved without any external hacker. The 128bits hashing value (i.e., a character series of 128bits) is generated for the content of the certificate, encrypted with the service server's secret key, and then appended to the certificate. When the mobile station receives the certificate, the mobile station takes the encrypted hash value and decrypts it with the public key of the service server. Then, to verify that the

certificate has not been tampered with, the mobile station generates the certificate hash value again and compares it with the decrypted hash value – if both match, the certificate is valid. Accordingly, a secure hash value is used to authenticate messages, and to ensure that the data sent from the service server is not tampered en-route. Then, it is verified that the public key of the web server is valid to perform the step 324.

Although the previous description concerns the user's information transmitted from the mobile station to the web server, it also applies to the opposite transmission of the user's information requiring security. In this case, the mobile station may likewise decipher the enciphered information from the web server using the public key and the secret key.

In addition, the security transaction application program for the mobile station and web server is prepared as described below.

Firstly, the HTML document for securing the user's information by enciphering/deciphering is prepared and uploaded to the web server. The distinction by the Internet search engine between the HTML documents requiring enciphering/deciphering from the ordinary HTML document is made by using the class attribution defined in the Internet web protocol. This may be achieved by designating the class as the security indicator "SCURE," which represents the corresponding field to be enciphered.

Thus, this invention provides an apparatus for securing the user's information for electronic trade in the mobile Internet communications.

While the present invention has been described in connection with specific embodiments accompanied by the attached drawings, it will be readily apparent to those skilled in the art that various changes and modifications may be made thereto without departing from the gist of the present invention.

WHAT IS CLAIMED IS:

1. A security system comprising at least one mobile station, an Internet service server, and a web server, said mobile station being operative to transmit/receive data to/from said web server via said Internet service sever; characterized in that, upon request for transmission of said data by said mobile station or said web server, said data is enciphered in a predetermined format to be transferred to one of said mobile station or said web server, said enciphered data is deciphered by one of said mobile station or said web server, without further intervention by said Internet service server.

2. The system as defined in Claim 1, wherein said service server registers in advance the certificate of said web server to be sent to said mobile station so that a previously registered certificate stored in said mobile station is updated when said mobile station requests a connection to said web server.

3. The system as defined in Claim 1, wherein said data is selectively enciphered/deciphered according to a class attribution of said request for the transmission of said data made by said mobile station or said web server.

4. The system as defined in Claim 4, wherein said enciphering/deciphering of said data is performed according to a Riverst-Shamier-Adleman (RSA) public key algorithm RSA algorithm and a SEED symmetric key algorithm, said SEED symmetric key algorithm is based on a Korean Data Encryption Standard developed by a Korea Information Security Agency (KISA).

5. A system for securing personal information exchanged during a security transaction in a mobile Internet communication system, comprising:

a web server for providing electronic data in response to a request by a user and for generating a public key and a secret key to secure said personal information;

a mobile station for generating a session key used in said security transaction using said public key received from said web server and for enciphering/deciphering said personal information using said session key; and,

wherein said web server deciphers said session key received from said mobile station using said secret key; and,

wherein said personal information enciphered by said mobile station is deciphered using said deciphered session key.

6. The system as defined in Claim 5, further comprising a service server for directly transmitting said personal information enciphered between said mobile station and said web server without further intervention by said service server.

7. The system as defined in Claim 5, wherein said enciphering/deciphering of said personal information by said session key is performed according to a Riverst-Shamier-Adleman (RSA) public key algorithm RSA algorithm and a SEED symmetric key algorithm, said SEED symmetric key algorithm is based on a Korean Data Encryption Standard developed by a Korea Information Security Agency (KISA).

8. A method for securing personal information transmitted from a mobile station of a mobile communications system in communication with a web server via a service server, comprising the steps of:

receiving a request for the transmission of said personal information from said mobile station or said web server;

selectively enciphering said personal information in a predetermined format to be transferred to one of said mobile station or said web server; and,

deciphering said enciphered personal information by one of said mobile station or said web server without having any intervention by said service server.

9. The method as defined in Claim 8, further comprising the step of transmitting a certificate from said Internet service server to said mobile station after receiving said request for the transmission of said personal information.

10. The method as defined in Claim 9, wherein said service server registers in advance said certificate of said web server to be sent to said mobile station so that a previously registered certificate stored in said mobile station is updated when said mobile station requests a connection to said web server.

11. The method as defined in Claim 8, wherein said data is selectively enciphered/deciphered according to a class attribution of said request for the transmission of said personal information made by said mobile station or said web server.

12. The method as defined in Claim 8, wherein said enciphering/deciphering of said personal information by said mobile station or said web server is performed according to a Riverst-Shamier-Adleman (RSA) public key

algorithm RSA algorithm and a SEED symmetric key algorithm, said SEED symmetric key algorithm is based on a Korean Data Encryption Standard developed by a Korea Information Security Agency (KISA).

13. A method for securing personal information transmitted from a mobile station of a mobile communications system in communication with a web server via a service server, comprising the steps of:

generating, by said web server, a public key and a secret key in response to a request made by a user to transmit electronic data, said public key and said secret key is used to secure said electronic data traveling to and from said mobile station;

transmitting said public key to said mobile station;

generating, by said mobile station, a session key responsive to said public key received from said web server, said session key is used for enciphering/deciphering said personal information transmitted between said mobile station and said web server; and,

wherein said web server deciphers said session key received from said mobile station using said secret key; and,

wherein said personal information enciphered by said mobile station is deciphered using said deciphered session key.

14. The method as defined in Claim 13, further comprising the step of transmitting, by said service server, said personal information enciphered between said mobile station and said web server without further intervention by said service server.

15. The method as defined in Claim 13, wherein said enciphering/deciphering of said personal information by said session key is performed according to a Riverst-Shamier-Adleman (RSA) public key algorithm RSA algorithm and a SEED symmetric key algorithm, said SEED symmetric key algorithm is based on a Korean Data Encryption Standard developed by a Korea Information Security Agency (KISA).

16. A method for securing data transmitted in a mobile Internet communications system of the type having a web server, a mobile station for exchanging data with said web server, and a proxy service server in communication with said mobile station and said web server, comprising the steps of:

requesting, by said mobile station, a connection to receive an electronic data from said web server via said service server;

generating, by said web server, a public key and a secret key in response to said

request by said mobile station;

transmitting, by said web server, said public key to said mobile station to be registered in said mobile station;

transmitting, by said service server, a new certificate to said mobile station;

determining, by said mobile station, whether a previously registered certificate in said mobile station is same as said new certificate received from said service server;

if said new certificate is same as said previously registered certificate, enciphering, by said mobile station, personal information using a session key generated by said public key received from said web server, and enciphering said public key to generate a symmetric key, and transmitting said enciphered personal information and said generated symmetric key to said web server via said service server; and,

deciphering, by said web server, said symmetric key received from said mobile station to covert back to said session key, and deciphering said enciphered personal information using said converted session key and said secret key.

17. The method as defined in Claim 16, further comprising the step of requesting, by said mobile station, said new certificate from said service server if said new certificate is not same as said previously registered certificate

18. The method as defined in Claim 16, further comprising the steps of enciphering, by said web server, the data transmitted to said mobile station using said symmetric key received from said mobile station; transmitting said enciphered data to said mobile station; and, deciphering, by said mobile station, said enciphered data received from said web server using said symmetric key transmitted previously to said web server.

19. The method as defined in Claim 16, wherein said enciphering/deciphering of said personal information by said session key is performed according to a Riverst-Shamier-Adleman (RSA) public key algorithm RSA algorithm and a SEED symmetric key algorithm, said SEED symmetric key algorithm is based on a Korean Data Encryption Standard developed by a Korea Information Security Agency (KISA).

FIG. 1

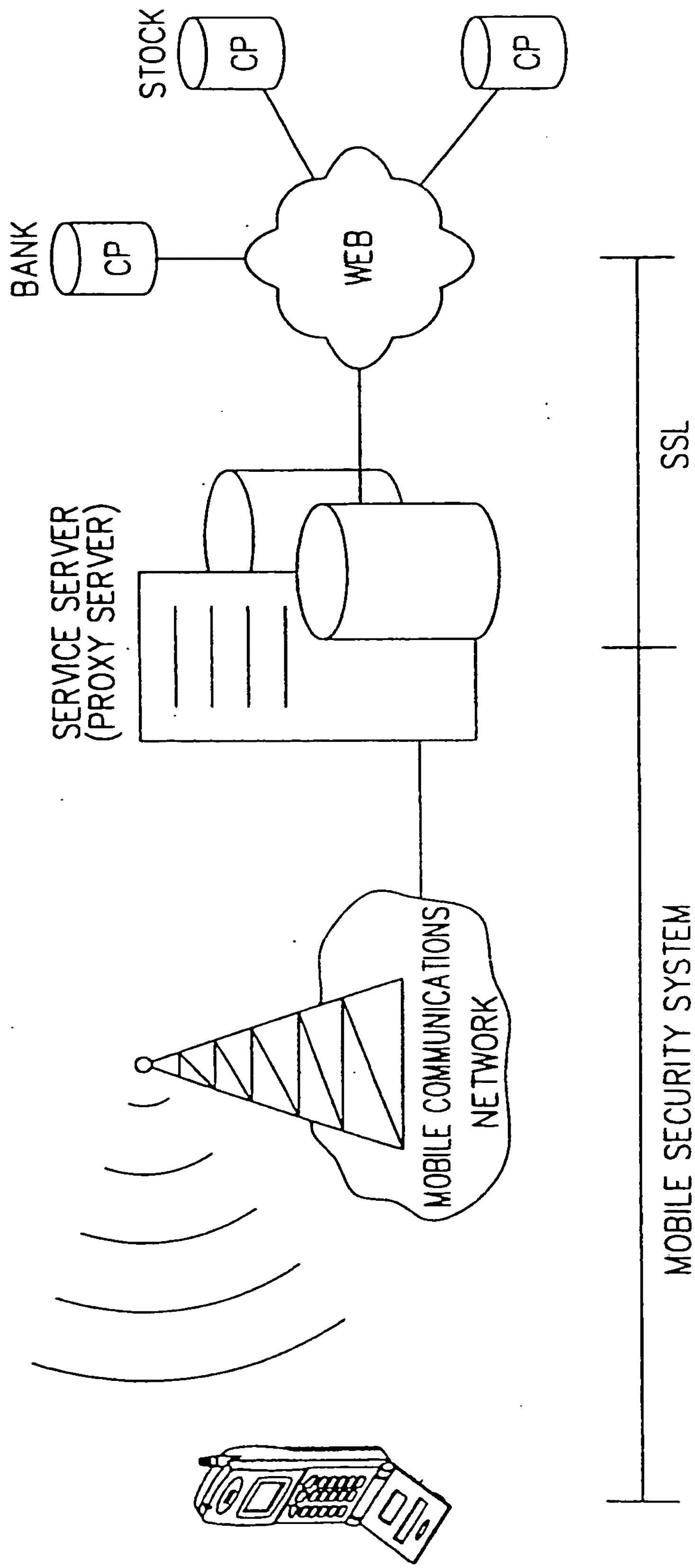

STOCK
CP
CP
BANK
CP
WEB
SERVICE SERVER
(PROXY SERVER)
SSL
MOBILE COMMUNICATIONS
NETWORK
MOBILE SECURITY SYSTEM

FIG. 2

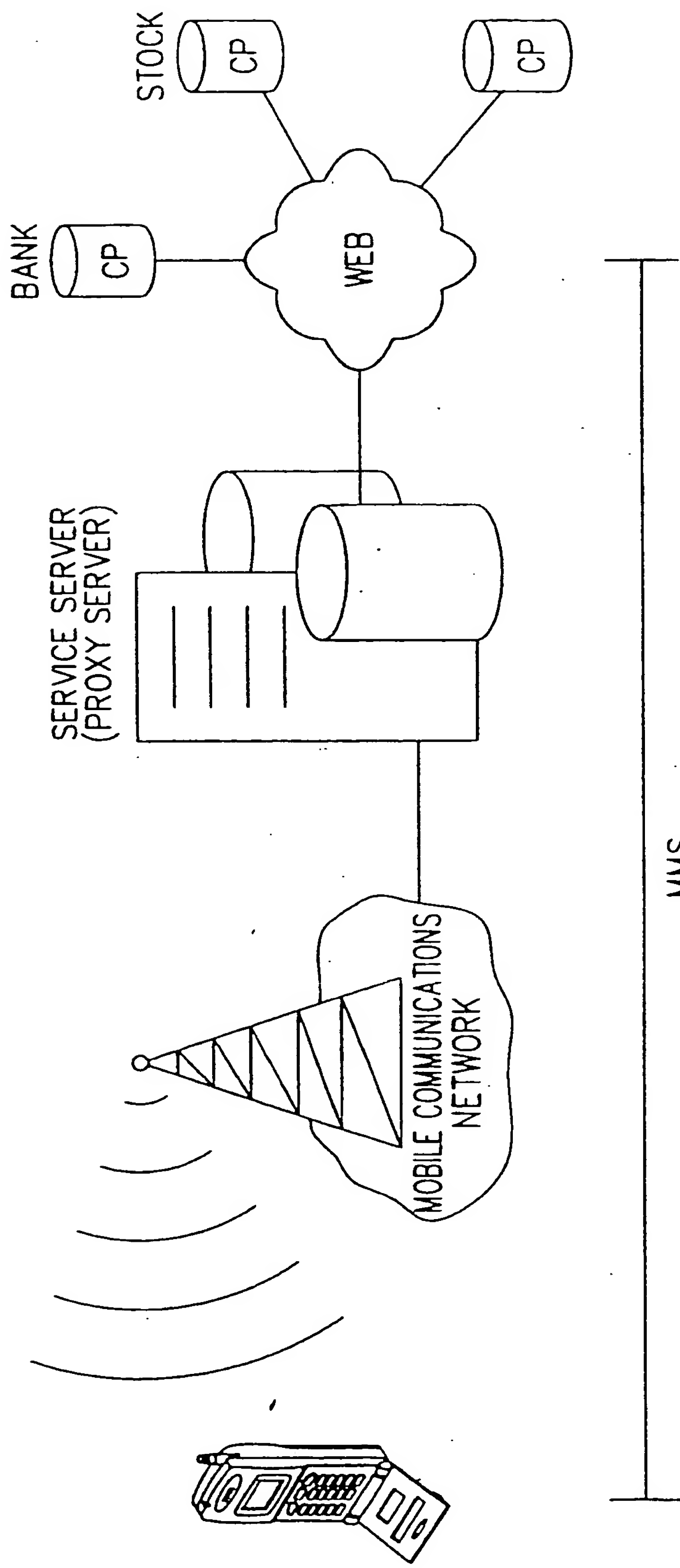
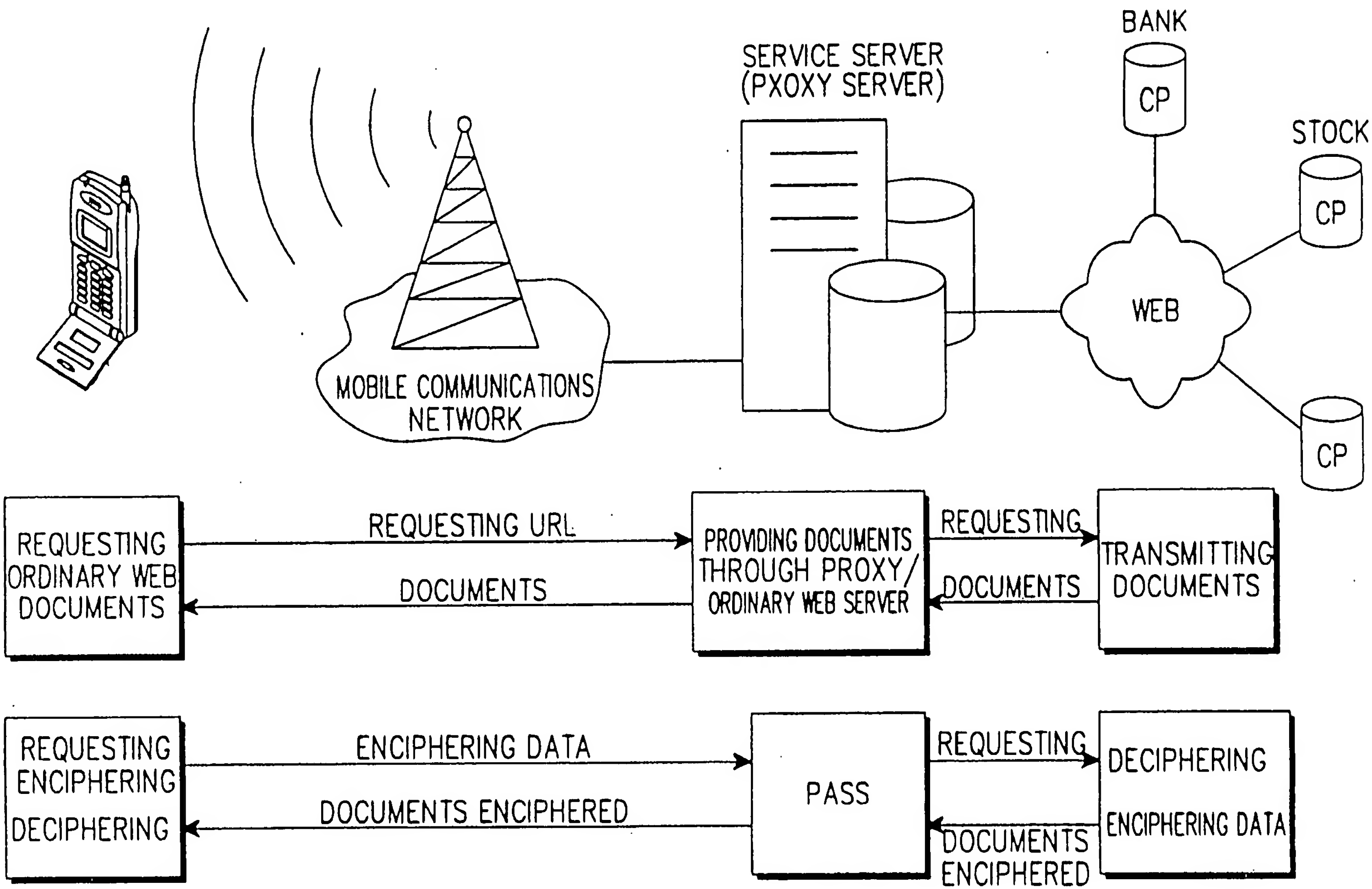

STOCK
CP
CP
BANK
CP
WEB
SERVICE SERVER
(PROXY SERVER)
MOBILE COMMUNICATIONS
NETWORK
MMS

FIG. 3


BANK
CP
STOCK
CP
CP
WEB
SERVICE SERVER
(PXOXY SERVER)
MOBILE COMMUNICATIONS NETWORK
REQUESTING ORDINARY WEB DOCUMENTS
REQUESTING URL
DOCUMENTS
PROVIDING DOCUMENTS THROUGH PROXY/ ORDINARY WEB SERVER
REQUESTING
DOCUMENTS
TRANSMITTING DOCUMENTS
REQUESTING ENCIPHERING
DECIPHERING
ENCIPHERING DATA
DOCUMENTS ENCIPHERED
PASS
REQUESTING
DOCUMENTS ENCIPHERED
DECIPHERING
ENCIPHERING DATA

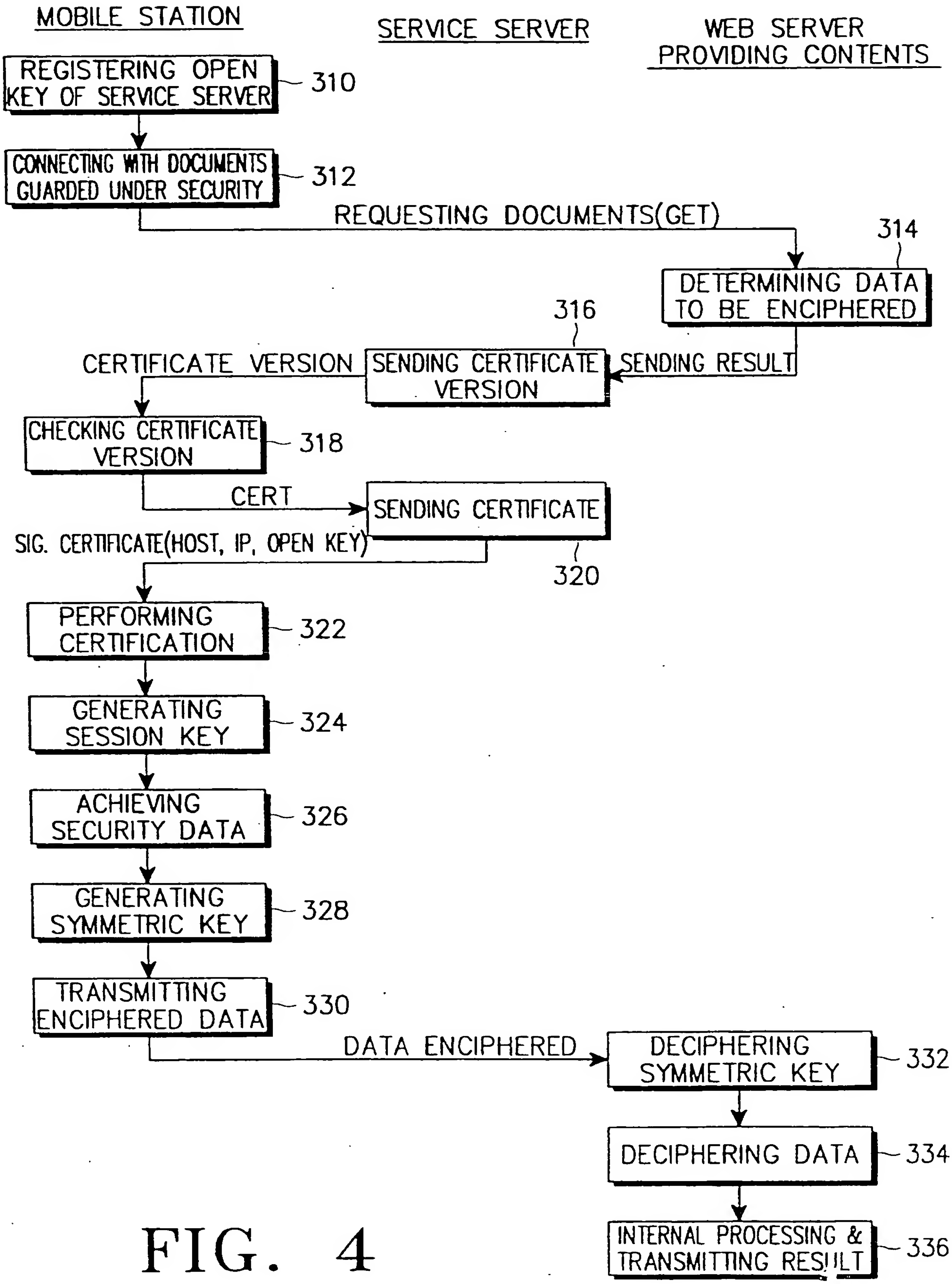

MOBILE STATION
SERVICE SERVER
WEB SERVER PROVIDING CONTENTS
REGISTERING OPEN KEY OF SERVICE SERVER
310
CONNECTING WITH DOCUMENTS GUARDED UNDER SECURITY
312
REQUESTING DOCUMENTS(GET)
314
DETERMINING DATA TO BE ENCIPHERED
316
CERTIFICATE VERSION
SENDING CERTIFICATE VERSION
SENDING RESULT
CHECKING CERTIFICATE VERSION
318
CERT
SENDING CERTIFICATE
SIG. CERTIFICATE(HOST, IP, OPEN KEY)
320
PERFORMING CERTIFICATION
322
GENERATING SESSION KEY
324
ACHIEVING SECURITY DATA
326
GENERATING SYMMETRIC KEY
328
TRANSMITTING ENCIPHERED DATA
330
DATA ENCIPHERED
DECIPHERING SYMMETRIC KEY
332
DECIPHERING DATA
334
INTERNAL PROCESSING & TRANSMITTING RESULT
336

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR00/00689

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 H04L 12/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimun documentation searched (classification system followed by classification symbols)

IPC7 H04L 9/00, H04L 9/32, H04B 7/26, H04L 12/66

Documentation searched other than minimun documentation to the extent that such documents are included in the fileds searched

Korean Patent ad applications for inventions since 1975

Electronic data base consulted during the intertnational search (name of data base and, where practicable, search trerms used)

WPI, JAPIO, USPTO, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 95/01,684 A(MOTOROLAR INC.) 12 JAN 1995 CLAIM 1, 6, 10	1-3, 5-6, 8-11, 13-14, 16-18
A	WO 94/16,516 A(AMERITECH CORP) 21 JUL 1994 ANTIRE DOCUMENT	1, 5, 8, 13, 16
A	US 5,371,794 A (SUN MICRO SYSTEM INC) 6 DEC 1994 ANTIRE DOCUMENT	1, 5, 8, 13, 16
A	KR 1999-86998 A (PITER F. KING) 15 DEC 1999 ANTIRE DOCUMENT	1, 5, 8, 13, 16

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevence

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevence: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevence: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 AUGUST 2000 (29.08.2000)	30 AUGUST 2000 (30.08.2000)

36

Name and mailing address of the ISA/KR
Korean Industrial Property Office
Government Complex-Taejon, Dunsan-dong, So-ku, Taejon Metropolitan City 302-701, Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer
MA, Jung Youn
Telephone No 82-42-481-5707

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/KR00/00689

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 95/01,684 A	12.01.95	PCT/US 94/05726	23.04.94
WO 94/16.516 A	21.07.94	US 36393A	04.01.93
		CN 1094882A	09.11.94
		US 5325419A	28.06.94
US 5,371,794 A	06.12.94	US 14766193A	02.11.93
		EP 0651533A2	03.05.95
		JP 7193569 A	28.07.95
		US 5371794A	06.12.94
KR 1999-86998 A	15.12.99	NONE	